# Case Study

## Testing physical security with red teaming

Visit: www.pgitl.com
Email: findoutmore@pgitl.com

Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK

PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865

# Summary

Our client engaged us to simulate a realistic physical intrusion exercise (red teaming) to test the resilience of their onsite security and whether a threat actor could gain access to sensitive areas within their premises.

Using a tailored social engineering approach, we were able to assess the effectiveness of the client's security controls including their employees' response. We demonstrated how critical assets could still be compromised with existing controls in place.

The engagement highlighted how human behaviour combined with unidentified gaps in physical security, can be leveraged to achieve unauthorised access. It provided the client with clear, actionable insight to close social engineering training gaps and strengthen their physical security posture.



Visit: www.pgitl.com
Email: findoutmore@pgitl.com
Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK
PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865

## The Brief

The client sought to validate and enhance their physical security posture by testing it against realistic attack scenarios. They wanted to identify and address any vulnerabilities that could allow a threat actor to gain physical access to their premises, including their lab and server.

After initial consultation, we defined the key objectives as:

- Assess the effectiveness of current processes and employee behaviour against an unauthorised access attempt.
- Test whether sensitive areas, including server infrastructure, are appropriately protected in practice.
- Determine how much access an unauthorised individual could realistically obtain and in what timeframe.
- Assess the effectiveness of front-of-house and entry-point security controls.



## Our Solution

We designed a bespoke red teaming engagement using social engineering techniques, reflecting how modern threat actors combine information gathering, manipulation and human interaction to bypass traditional controls.

Leveraging a media engagement pretext, we created a realistic podcast concept and outreach campaign. This approach enabled us to:

- Engage transparently with the organisation through a plausible business context.
- Experience the visitor journey end-to-end.
- Observe how the organisation's security controls operate under normal conditions.

To ensure authenticity, we developed detailed personas and rehearsed the engagement, allowing for natural interactions and meaningful assessment of real-world behaviours.

## The Challenge

To ensure the exercise remained realistic and valuable, we operated under conditions that genuine threat actors would be up against, which included:

- Limited initial intelligence, requiring adaptive planning and flexible execution
- Authentic scenario delivery, including running a credible podcast engagement
- Discreet onsite coordination, reflecting real-world operational constraints

These factors ensured the findings accurately represented how the organisation's controls would perform in a real-world scenario, going beyond a theoretical testing environment.



## The Results

The engagement provided the client with practical insights into their physical security resilience including:

- **Effective engagement processes:** Onsite staff were open, professional and collaborative, supporting a positive visitor experience.
- **Control validation:** The exercise demonstrated how existing controls function in practice across the site.
- **Opportunities for enhancement:**
  - Identifying any gaps in current processes and controls
  - Strengthening access control around sensitive assets
  - Reducing reliance on easily discoverable physical security measures (e.g., keys, padlocks)
  - Reinforcing escalation pathways where concerns arise

## Client testimonial

"PGI were very flexible and patient around some of our hectic diary management, and very clear in what they were doing and how the project would progress. We understood the parameters and the red lines that you wouldn't cross (e.g., you wouldn't cause damage as part of the exercise) and had absolute clarity throughout.

From an exercise point of view, there was nothing that could have been improved. The engagement definitely provided value to our organisation. Our internal security outcome provided us with valuable insights to strengthen our controls and address social engineering training gaps."

**Chief Financial Officer**

Visit: www.pgitl.com
Email: findoutmore@pgitl.com
Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK
PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865